WHAT IS CLAIMED IS:

1. A method of allowing an employee associated with a first enterprise to access a first Intranet owned by the first enterprise from a computing device located within a semiconductor fabrication facility in which a plurality of client systems located within said facility are connected to a second Intranet using a first physical connection type, said fabrication facility, plurality of client systems and second Intranet all being owned by a second enterprise, said method comprising:

connecting said computing device to said second Intranet through a node using a second physical connection type that is different from said first physical connection type;

establishing an isolation pipe through said second private Intranet between said node and a hub using virtual private network technology;

generating a request to logon to said first Intranet from said computing device;

formatting said request in a secure Internet protocol such that said request is broken up into multiple standard Internet packets, where each packet includes at least a network transmission header portion and an encrypted data portion; and

transmitting said formatted request through said isolation pipe over said second Intranet to said hub and then through a firewall and over the public Internet to said first Intranet.

2. The method of claim 1 wherein said formatted request is received at the first private Intranet.

3. The method of claim 1 wherein said formatted request is transmitted through said isolation pipe using a tunneling protocol selected from the group consisting of: layer 2 tunneling protocol, point-to-point tunneling protocol, layer 2 forwarding and generic routing encapsulation.

4. The method of claim 1 wherein said formatted request is encrypted using a Secure Sockets Layer (SSL) encryption protocol.

5. The method of claim 5 wherein both the network transmission header and already encrypted data portions of each packet associated with said formatted request is encrypted at said node using a VPN-level encryption protocol prior

to being transmitted through said isolation pipe and then decrypted at said hub/firewall such that the header is unencrypted and the data portion is encrypted using only the SSL protocol prior to being transmitted over the public Internet.

6. The method of claim 1 wherein said first enterprise is a semiconductor equipment manufacturer.

7. The method of claim 1 wherein said computing device is connected to said second Intranet from inside a cleanroom.

8. In a customer network comprising a plurality of customer client systems, at least one customer server system and a customer firewall where said plurality of customer client systems are communicatively coupled to said server system using a first physical connection type, said server system is communicatively coupled to said firewall and said customer firewall is communicatively coupled to a public network, a method of allowing end-to-end secure communication from a supplier client system located behind said firewall to a supplier server system accessible over said public network, said method comprising:

connecting said supplier client system to said customer network using a second physical connection type that is different from said first physical connection type;

establishing an isolation pipe between said supplier client system and a server system of said customer network through use of a tunneling protocol;

transmitting data from said supplier client system through said customer network and towards said firewall using said isolation pipe;

transmitting said data from said customer firewall to said public network; and

receiving said data at said supplier server system.

9. The method of claim 8 further comprising:

in response to receiving said data at said supplier server system, transmitting data from said supplier server system to said supplier client system.

10. The method of claim 9 wherein the public network is the Internet and wherein data from said supplier system that is transmitted through said customer network is formatted in a secure Internet protocol such that said data is broken up into

multiple standard Internet packets, where each packet includes at least a network transmission header portion and an encrypted data portion.

11. The method of claim 10 wherein said secure Internet protocol is the Secure Sockets Layer (SSL) protocol.

12. The method of claim 11 wherein said isolation pipe through said customer network is established by a virtual private network hub and a virtual private network node and said supplier client system is connected to said customer network through said virtual private network hub.

13. A method for allowing end-to-end secure communication over a public network from a client system located behind a firewall of a first private network to a server system associated with a second private network, said method comprising:

authenticating communication between said client system and a wireless access point of said first private network;

thereafter, generating, from said client system, a request for a Web page stored on said server system;

transmitting said request from said client system to server system by routing said request through said first private network, over said public network and then to said second private network, wherein said request is routed through said first private network, in order, from said client system, to said wireless access point, to a virtual private network node, to a virtual private network hub, and through said firewall and wherein said request is routed from said virtual private network node to said virtual private network hub using a tunneling protocol.

14. The method of claim 13 wherein said client system is located in a cleanroom of a semiconductor fabrication facility and said wireless access point is located outside said cleanroom.

15. A networked system comprising:

a private communication network;

a supplier client system coupled to the private network;

a firewall coupled to the network, said firewall providing security features that enable said private network to connect to a public network; and

a virtual private network system, coupled to the private network;

wherein said virtual private network system is configured to:

receive a request from said supplier client system for viewing a desired Web page sent over the public network, create a secure pipeline within said private communication network tunnel to transmit said request from said supplier client system to said firewall and transmit said desired Web page from said Internet through said firewall to said supplier client system.

16. The system of claim 15 wherein said supplier client system is configured to generate said request in a secure Internet protocol such that said request is broken up into multiple standard Internet packets, where each packet includes at least a network transmission header portion and an encrypted data portion.

17. The system of claim 16 wherein said virtual private network system comprises at least a VPN node and a VPN hub, and wherein said supplier client system is coupled to said private network through said VPN node and said VPN node directs communications through said private network directly to said VPN hub.

18. The system of claim 17 wherein said VPN node is configured to transmit only requests generated in said secure Internet protocol to said VPN hub.

19. The system of claim 18 wherein said secure Internet protocol is the Secure Sockets Layer (SSL) protocol.

20. A networked system comprising:

a private communication network;

a virtual private network (VPN) node coupled to said private network;

a supplier client system coupled to the private network through said VPN node;

a VPN hub coupled to said private network, wherein said VPN node and VPN hub are configured to create an isolation pipe therebetween within said private network;

a firewall coupled to the private network, to said VPN hub and to a public network, said firewall providing security features that enable said private network to connect to the public network.

21. The networked system of claim 20 wherein:

said VPN node is configured to receive a request from said supplier client system for viewing a desired Web page sent over the public network and pass said request on to said VPN hub using a tunneling protocol;

said VPN hub is configured to pass said request from said VPN node to towards said firewall; and

said firewall is configured to transmit said request over said public network.

22. The system of claim 21 wherein said VPN node is configured to transmit only requests generated in said secure Internet protocol to said VPN hub.

23. The system of claim 22 wherein said secure Internet protocol is the Secure Sockets Layer (SSL) protocol.